United Nations A/C.3/55/L.8

General Assembly

Distr.: Limited
5 October 2000

Original: English

Fifty-fifth session
Third Committee
Agenda item 105
Crime prevention and criminal justice

Australia, Austria, Belgium, Canada, Chile, Colombia, France, Germany, Ireland, Luxembourg, Spain, Sweden, Netherlands, United Kingdom of Great Britain and Northern Ireland and United States of America: draft resolution

Combating the criminal misuse of information technology

The General Assembly,

Recalling the role of the United Nations in the promotion of international peace and security, and deeply concerned by the threats posed to international peace and security by the criminal misuse of information technology,

Emphasizing the contributions that the United Nations can make in the area of crime prevention and criminal justice, as well as in the promotion of more efficient and effective law enforcement and administration of justice, and of the highest standards of fairness and human dignity,

Recognizing that the free flow of information can promote democratic governance, education and economic and social development,

Noting significant advancements in the development and application of information technology and means of telecommunication,

Expressing concern that technological advancements have created new opportunities for criminal activity,

Noting that widespread reliance on information-based technology has resulted in a substantial increase in global cooperation and coordination, with the result that criminal misuse of information technology may have a grave impact on all States,

Committed to the maintenance of international stability through closer coordination and cooperation among States in combating crime, including criminal and terrorist acts involving and facilitated by computer networks and other information technology, and bearing in mind the role that can be played by both the United Nations and regional organizations in this respect,

00-67689 (E) 061000

Recalling its resolutions 53/70 of 4 December 1998 and 54/49 of 1 December 1999 regarding the misuse and exploitation of information technology for criminal or terrorist purposes and the response of States to these resolutions, emphasizing the need to focus efforts on combating criminal and terrorist use of information technology,

Reaffirming the need to prevent the misuse or exploitation of information technology for criminal purposes,

Recognizing the need for cooperation between States and private industry in combating the criminal and terrorist misuse of information technology,

Welcoming the work of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held at Vienna from 10 to 17 April 2000, the work of the Subgroup of the Group of Eight on high-tech crime and, notably, of the Conference of the Group of Eight on a dialogue between government and industry on safety and confidence in cyberspace, held in Paris from 15 to 17 May 2000, the work of the Government Experts on Cybercrime, convened by the Organization of American States and the work of the Committee of Experts on Crime and Cyberspace of the Council of Europe on a draft convention on cybercrime,

Welcoming the principles agreed to by the Ministers for Foreign Affairs of the Group of Eight in Washington, D.C., on 10 December 1997, which were endorsed by the Heads of State of the Group of Eight, meeting at Birmingham, United Kingdom of Great Britain and Northern Ireland, in May 1998, and the communiqué issued by the Ministers for Foreign Affairs of the Group of Eight in Moscow on 20 October 1999, which was endorsed by the Heads of State of the Group of Eight, meeting at Okinawa, Japan in July 2000,

Welcoming also the recommendations approved in resolution AG/RES.1615 (XXIX-0/99) of 2 March 2000, by the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, convened in Costa Rica within the framework of the Organization of American States,

1. *Commends* the efforts of the bodies mentioned above to prevent the misuse of information technology and takes note of the value of, inter alia, the following principles to combat cybercrime and to protect the freedom of information and development:

(a) There must be no safe haven for those who abuse information technologies;

(b) The investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where the harm has occurred;

(c) Information should be exchanged among States regarding the problems that they confront in combating high-tech crime;

(d) Law enforcement personnel must be trained and equipped to address high-tech crime;

(e) Legal systems must protect the confidentiality, integrity and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized;

(f) Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime;

(g) Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime;

(h) Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State in which the data are located;

(i) The general public should be made aware of the need to prevent and combat high-tech crime;

(j) Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed;

(k) To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence;

(l) The fight against the illegal use of information and communication technology requires the development of solutions, taking into account both the protection of individual freedoms and private life and the preservation of the ability of Governments to fight high-tech crime;

2. *Urges* States to take all appropriate steps to implement the principles mentioned above;

3. *Decides* to maintain the question of cybercrime on the agenda of its fifty-sixth session, as part of the item on crime prevention and criminal justice.